OULUN SEUDUN
AMMATTIKORKEAKOULU

Petri Savolainen

KERTAKÄYTTÖSALASANAJÄRJESTELMÄ YRITYKSEN VERKKOON KIRJAUTUMISESSA

KERTAKÄYTTÖSALASANAJÄRJESTELMÄ YRITYKSEN VERKKOON KIRJAUTUMISESSA

Petri Savolainen
Opinnäytetyö
Kevät 2013
Tietojenkäsittelyn koulutusohjelma
Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

Tekijä: Petri Savolainen
Opinnäytetyön nimi: Kertakäyttösalasanajärjestelmä yrityksen verkkoon kirjautumisessa
Työn ohjaaja: Jukka Kaisto
Työn valmistumiskuukausi ja -vuosi: Kevät 2013 Sivumäärä: 29

Opinnäytetyön tarkoituksena oli ottaa käyttöön kertakäyttösalasanajärjestelmä oululaisen ICT-alan yrityksen SSL VPN -yhteyden todentamisvaiheeseen. Yritys oli ennen opinnäytetyön aloittamista päätynyt Entrust IdentityGuard -järjestelmään. Järjestelmän yhteyteen oli jo hankittu useita avaimenperänä toimivia token-laitteita, lisenssit tarvittavalle määrälle käyttäjiä sekä soft token -ohjelmistoihin.

Työn teoriaosuus käsittelee tietoturvaa ja niiden oheisjärjestelmien toimintaa, joita käyttöönotettava ratkaisu käyttää tai vaatii toimiakseen. Tietoturvasta käsitellään tarkemmin tietoturvan osa-alueita yrityksen tietoturvan kannalta, tietoturvapolitiikkaa sekä henkilön tunnistamista ja todentamista. Käytettäviä oheisjärjestelmiä ovat välityspalvelimet, hakemistopalvelut ja VPN-verkot.

Järjestelmän tarkoituksena on yrityksen tietoturvapolitiikan mukainen vahva todentaminen, kun yrityksen työntekijä käyttää yrityksen sisäverkon resursseja yrityksen tilojen ulkopuolelta. Ensimmäinen todentaminen suoritetaan RADIUS Proxyn kautta Active Directory hakemistopalvelussa ja toinen todentaminen suoritetaan IdentityGuard-järjestelmässä. Opinnäytetyön tuloksena yrityksessä on otettu käyttöön järjestelmä, joka kasvattaa yrityksen tietoturvan tasoa huomattavasti.

Avainsanat: Entrust, etäkäyttö, tietoturva, vahva todentaminen

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author: Petri Savolainen
Title of thesis: One-time password system on company private network sign-up
Supervisor: Jukka Kaisto
Term and year when the thesis was submitted: Spring 2013 Number of pages: 29

The aim of this thesis was to implement a one-time password system for SSL VPN connection authentication into operation for an ICT company located in Oulu. Before the beginning of this thesis the company had decided to use Entrust IdentityGuard system to provide strong authentication. For system operation the company had bought multiple token key rings, user access licenses for a required number of company employees and soft token software licenses.

The theoretical background of the thesis deals with data security and operation of required secondary systems witch the solution uses to operate. Data security is discussed in more detail regarding parts of data security in the company, data security policy as well as person identification and authentication. Operational secondary systems are proxy servers, directory services and VPN connections.

The main purpose of the system is obeying company security policy of strong authentication when an employee uses company private network resources from outside of company premises. The first step of authentication is performing authentication from Active Directory. The second step is completing authentication in IdentityGuard system. As a result of this thesis the company has taken into use a system that raises the level of data security significantly.

Keywords: Entrust, remote access, data security, strong authentication

SISÄLLYS

1 JOHDANTO 6
2 YRITYKSEN TIETOTURVA 7
2.1 Tietoturvan päämäärät 7
2.2 Tietoturvapolitiikka 8
2.3 Tunnistautuminen 9
2.3.1 Tunnistus 9
2.3.2 Todennus 11
2.3.3 Hakemistopalvelu 11
2.3.4 Välityspalvelin 12
2.4 Salaus 13
3 VIRTUAL PRIVATE NETWORK 15
3.1 Tunnelointi 15
3.2 SSL VPN 16
4 KÄYTTÖÖNOTTO 17
4.1 Verkkoympäristö 17
4.2 Kertakäyttösalasanajärjestelmä 17
4.3 Asennuksen vaiheet 21
4.4 Käyttöönotto VPN-kirjautumisessa 22
5 HALLINTA 23
5.1 Käyttäjän lisääminen järjestelmään 23
5.2 Lisenssitietojen tarkastaminen 24
6 POHDINTA 25
LÄHTEET 27

1 JOHDANTO

Opinnäytetyö tehtiin oululaiselle ICT-alan yritykselle, jossa oli päätetty ottaa käyttöön vahva todentaminen käytettäessä yrityksen sisäverkon resursseja julkisesta verkosta. Tarkoituksena oli ottaa yrityksen tietoturvapolitiikassakin mainittu kaksivaiheinen todentaminen käyttöön työntekijän kirjautuessa SSL VPN -yhteyteen. Yritys oli ennakkoselvitysten perusteella päätynyt Entrust IdentityGuard -järjestelmään, jolla järjestelmä myös toteutettiin. Opinnäytetyössä on käsitelty Entrust IdentityGuard -järjestelmän käyttöönotto ja hallinta.

Opinnäytetyössä käsitellään yrityksen tietoturvaa ja tietoturvapolitiikkaa, todentamista, salaamista sekä VPN-yhteyksiä. Yrityksen tietoturvassa käsitellään tietoturvan päämääriä sekä tietoturvapolitiikan tarkoitusta. Todentamisesta käydään läpi henkilön tunnistamista ja todentaminen perustuen kolmeen päämäärään: jotain mitä henkilö tietää, mitä hänellä on hallussaan tai yksilöllinen ominaisuus. Työssä käsitellään myös hakemistopalvelun ja välityspalvelimen merkitystä. Salaamisessa otetaan kantaa salaamisen käyttötarkoitukseen ja salausmenetelmiin. VPN-yhteys käsitellään SSL VPN -tekniikan osalta.

Opinnäytetyön aihe on hyvin ajankohtainen tietoverkkojen turvattomuuden ja tietoturvaloukkausten yleistyessä. Yrityksissä käsitellään hyvin arkaluonteisia asioita eikä tietojen haluta leviävän ulkopuolisten käsiin tahallisesti tai tahattomasti. Työ opettaa eri todennus- ja salausmenetelmistä sekä VPN-tekniikoista. Kertakäyttösalasanajärjestelmiä otetaan tulevaisuudessa käyttöön yleisemminkin tietoturvatietouden lisääntyessä.

2 YRITYKSEN TIETOTURVA

”Tietoturvan tavoitteena on turvata tietojenkäsittelyn toimivuus erilaisia uhkia vastaan, sekä suojata tietoja oikeudettomilta muutoksilta.” Ihmisten toiminta on tietoturvan kannalta suurin uhka. (Järvinen 2003, 29.)

Kaiken suojauksen perusperiaatteena on tarjota käyttäjille vain välttämättömät oikeudet tarvitsemiinsa laitteisiin ja niiden sisältämiin tietoihin. Verkon haltijan tulee tuntea hyvin organisaation toimintaprosessit ja niiden vaikutukset tietojenkäsittelyyn. Verkon, kuten koko tietojärjestelmän, suunnittelussa tulee pitää lähtökohtana organisaation toimintaprosesseja sekä niiden tiedontarpeita. Tietoturvasuunnitelma on aina vain kompromissi palvelutekijöiden ja uhkatason välillä. (Hakala & Vainio 2005, 343.)

Yrityksen omat työntekijät voivat tehdä vakavia virheitä kiireen, välinpitämättömyyden tai osaamattomuuden vuoksi. Ulkopuoliset henkilöt voivat hankkia luottamuksellista tietoa tai vahingoittaa tietojärjestelmien toimintaa. Yksi helppo tapa tietojen kaappaamiseen on esimerkiksi soittaa väärällä identiteetillä yrityksen työntekijälle, joka hyväuskoisuuttaan luovuttaa salasanan kaappaajalle. (Järvinen 2003, 29.)

2.1 Tietoturvan päämäärät

Tietoturvan päämääriä ovat luottamuksellisuus, eheys, saatavuus, pääsynvalvonta, kiistämättömyys ja todennus (Järvinen 2003, 30–33). Tiedon eheys, oikea alkuperä ja luottamuksellisuus varmistetaan tietojen arkaluonteisuuden mukaan soveltuvilla salaus- tai allekirjoitusteknologioilla (Valtiovarainministeriö 2012, 90).

Luottamuksellisuus tarkoittaa, että tietoon on pääsy vain siihen oikeutetuilla henkilöillä (Järvinen 2003, 30–33). Käyttäjälle kerrotaan mitä ja miten tietoa hänestä kerätään ja mihin tarkoitukseen niitä käytetään. Käyttäjälle tarjotaan myös mahdollisuus vaikuttaa hänestä kerättäviin tietoihin. (Valtiovarainministeriö 2012, 89.)

Eheys on tiedon ominaisuus, joka ilmentää sitä, että tiedon sisältö ei ole muuttunut sen siirron tai säilytyksen aikana. Pyrkimyksenä tällä on tiedon ja sen käsittelytapojen virheettömyys (Sanastokeskus TSK ry 2004, 11; Oulun yliopisto: Tietohallinto 2013, hakupäivä 13.4.2013.)

Tiedon muuttumisella tarkoitetaan tiedostojen poistoa tai asiatonta muokkausta. Eheyden uhkana ovat esimerkiksi virukset tai tahattomasti laiterikko. (Oulun yliopisto: Tietohallinto 2013, hakupäivä 13.4.2013.)

Saatavuudella tarkoitetaan lähinnä teknisiä seikkoja, kuten esimerkiksi varmuuskopiot ja luotettavat verkkoyhteydet. Saatavuus on ainut tietoturvaperiaate, johon ei voida hyödyntää salausta. (Järvinen 2003, 30–33.) Saatavuutta kutsutaan usein myös käytettävyydeksi. Tällä tarkoitetaan tiedon saatavuutta kohtuullisessa vasteajassa vain niille tarkoitetuiden henkilöiden saatavaksi ja käytettäväksi. (Oulun yliopisto: Tietohallinto 2013, hakupäivä 13.4.2013.)

Pääsynvalvonnalla varmistetaan tietojen saatavuus vain tunnistetuille käyttäjille tai henkilöille (Järvinen 2003, 30–33). Pääsynvalvontaa toteutetaan käyttöoikeuksin ja erilaisilla tunnistautumismetodeilla (Oulun yliopisto: Tietohallinto 2013, hakupäivä 13.4.2013).

Kiistämättömyydellä tarkoitetaan tietojärjestelmissä tehtyjen toimenpiteiden tutkimista jälkikäteen, mikä voi tarkoittaa esimerkiksi lokiseurantaa (Järvinen 2003, 30–33; Valtiovarainministeriö 2012, 90). Kiistämättömyydellä varmistetaan, ettei henkilö voi kiistää olleensa jossain tapahtumassa osapuolena. Kiistämättömyyden periaatteet liittyvät vahvasti todennukseen ja eheyteen. (Oulun yliopisto: Tietohallinto 2013, hakupäivä 13.4.2013.)

Todennuksella saavutetaan ihmisten henkilöllisyyden ja tekniikan (laitteet, ohjelmat) aitouden varmistaminen (Järvinen 2003, 30–33). Todennus edellyttää osapuolilta aina jotain yksilöllistä ominaisuutta (Oulun yliopisto: Tietohallinto 2013, hakupäivä 13.4.2013).

2.2 Tietoturvapolitiikka

Tietototurvapolitiikka voidaan määritellä usealla eri tavalla, mutta pääsääntöisesti se on organisaation johdon hyväksymä näkemys tietoturvan päämääristä, periaatteista, vastuista ja toteutuksesta. Tietoturva on osa yritysturvallisuutta eikä sitä voi eriyttää yrityksen muista turvakäytänteistä. Esimerkiksi kulunvalvonta sivuaa läheisesti tietoturvapolitiikkaa. Tietoturvapolitiikan on elettävä yrityksen mukana. Uusien järjestelmien käyttöönotossa on päivitettävä tietoturvapolitiikkaa päivityksien mukaiseksi. On myös huomioitava käytännöt ja ohjeistukset. (Hämäläinen 2005, hakupäivä 24.3.2013.)

”Tietoturvassa ei ole kyse vain tekniikasta, vaan ihmisten työskentelytavoista”. Yrityksen toiminnassa kaikkien tulee tietää tietoturvan huolehtimisesta. Joissain tiedoissa yrityksellä on

lainsäädännöllinen velvoite huolehtia turvaamisesta. Kaikki tärkeä tieto ei ole vain sähköisessä muodossa, vaan myös paperit ja puhuttu tieto on tärkeää. (Tietoturvaopas.fi 2013, hakupäivä 2.4.2013.)

Kehitettäessä turva-arkkitehtuuria tulee huomioida muutamia yleisiä alueita. On mietittävä, mitä resursseja tarvitsee suojata, mitä ongelmia (uhkia) vastaan suojaudutaan, ongelmien (uhkien) samankaltaisuus ja kuinka usein suunnitelmia uudelleenkatselmoidaan ja päivitetään. (McCabe 2008, 67.)

2.3 Tunnistautuminen

Kirjauduttaessa palveluihin käyttäjätunnuksella ja salasanalla on käytössä kaksi vaihetta. Ensin *tunnistetaan* nimen tai muun tunnisteen perusteella, kuka käyttäjä on kyseessä. Tunnistamisen jälkeen *todennetaan* käyttäjän salasanan perusteella, että käyttäjä on varmasti se, joka väittää olevansa. (Järvinen 2003, 204.)

Todennus palvelee kahta tarkoitusta. Todennus kelpuuttaa, että viestin lähettäjä tai vastaanottaja on se, kuka väittää olevansa sekä varmistaa viestin vastaanottamisen alkuperäisessä muodossaan. Sovellustasolla todennus suoritetaan pääsääntöisesti käyttäjätunnus-salasanaparin vaihdolla. (Farrel 2008, 117.)

2.3.1 Tunnistus

Käyttäjätunnus on käyttäjän sähköiseen tunnistamiseen käytettävä tunniste, jolla erotetaan käyttäjät toisistaan ja jota käytetään yleensä salasanan kanssa (Sanastokeskus TSK ry 2004, 21). Palveluun kirjautuessa palvelu tunnistaa käyttäjän aiemmin määritellyn tunnuksen perusteella. Käyttäjätunnus luodaan usein nimen alkukirjaimista, mutta tunnuksen luominen ei edellytä tätä. Monesti käyttäjätunnus on myös looginen, esimerkiksi *etunimi.sukunimi*. (Cibernarium 2005, hakupäivä 2.4.2013).

Hyvän salasanan keksiminen on vaikeaa, joten kaikkein turvallisimmassakin salaustekniikassa on ongelmia. Tämän lisäksi keksimisen pitäisi olla jatkuvaa, koska salasanoja tulisi vaihtaa säännöllisesti. Käyttäjät ovat usein mukavuudenhaluisia ja siksi on houkutus valita lyhyt, helposti muistettava salasana. Järjestelmiin on usein sisällytetty salasanavaatimuksia, joilla pakotetaan

käyttäjä valitsemaan salasanaansa esimerkiksi pieniä ja isoja kirjaimia sekä määritellään minimipituus. (Järvinen 2003, 244–247.)

Luonnollisen kielen sanat tai nimet ovat suosittuja valintoja salasanoiksi. Salasana ei kuitenkaan saisi olla tällainen, koska eri kielillä on saatavilla tuhansien sanojen mittaisia listoja, joita hyökkääjä voi kokeilla. Sanakirjahyökkäys ja brute-force edellyttää hyökkääjän pääsyä kokeilemaan sanoja kaikessa rauhassa. Kolmesta väärästä kirjautumisyrityksestä lukitseva järjestelmä on immuuni sanakirjahyökkäyksille. Salattuja työtiedostoja tai kaapattuja viestejä voi kuitenkin murtaa rauhassa. (Järvinen 2003, 244–247.) Salasanojen heikkous on uhkana tietoturvan päämäärissä luottamuksellisuudelle ja pääsynvalvonnalle.

Salasana tallennetaan usein järjestelmään jollain algoritmilla tehtynä yksisuuntaisena tiivisteenä. Jos hyökkääjä saa salasanojen tiivistelistan haltuunsa, hän voi verrata itse tuottamiaan tiivisteitä hankkimansa listan sisältöön ja selvittää näin salasanan. (Järvinen 2003, 244–247.) Salasanoja säilytetään yleensä hakemistopalvelussa, kuten esimerkiksi Active Directory.

Windows-käyttöjärjestelmät tallentavat salasanat yksisuuntaisena tiivisteenä kahdella eri tavalla: LAN Manager one-way function (LM OWF) ja NT OWF. LM OWF -algoritmi on Windows käyttöjärjestelmissä mukana taaksepäinyhteensopivuuden vuoksi ja nykyään Active Directory -ympäristössä käytetään NT-tiivistettä. (Microsoft 2012, hakupäivä 28.5.2013.)

LM OWF -tiiviste luodaan lisäämällä salasanaan NULL-tavuja, että salasanasta saadaan 14 merkin mittainen. Tämän jälkeen salasana konvertoidaan versaaleiksi ja jaetaan kahdeksi seitsemän tavun avaimeksi. Avaimet salataan, ketjutetaan yhteen ja tallennetaan LM tiivisteenä. NT OWF luodaan salasanasta MD4-tiivistealgoritmilla ja tallennetaan. Windowsin salasanoja ei käsitellä suolaamalla. Suola on salasanaan ennen tiivisteen luomista lisättävä lisämääre, joka vaikeuttaa valmiiksi laskettujen murtotaulukoiden käyttämistä. (Järvinen 2003, 244; Microsoft 2012, hakupäivä 28.5.2013.)

Windows tallentaa toimialueen käyttäjien salasanan tarkisteen heidän kirjautuessaan toimialueessa olevaan työasemaan. Tarkistetta käytetään, kun käyttäjä yrittää kirjautua samaan työasemaan uudestaan, joka ei enää ole yhteydessä toimialuepalvelimeen. Tarkiste luodaan ketjuttamalla NT-tiiviste ja käyttäjän käyttäjätunnus ja tekemällä yhdisteestä MD4-tiiviste. (Microsoft 2012, hakupäivä 28.5.2013.)

Suomessa on kehitetty hyvin matkapuhelimiin perustuvia tunnistusmenetelmiä. Matkapuhelimella tehty todennus on monessa tapauksessa tarpeeksi luotettava GSM-järjestelmässä olevan

tietoliikennesalauksen ja PIN-koodin tuoman suojan turvin. Kertakäyttöisiin tunnuksiin perustuva W-Login V0 -matkapuhelintodennus toimii käyttäjän ilmoittaman puhelinnumeron perusteella. Sovellus luo satunnaisen kertakäyttöavaimen, joka lähetetään tekstiviestillä käyttäjän puhelimeen. Käyttäjällä on verkkopalvelussa 60 sekuntia aikaa kirjoittaa salasanakenttään saamansa salasana, jonka jälkeen hän pääsee kirjautumaan palveluun. (Järvinen 2003, 42.) Uudemmalla mobiilivarmenteella voidaan allekirjoittaa sopumuksia esimerkiksi netti- tai puhelinpalveluissa. Mobiilitunnistautuminen toimii muun muassa kansalaisen tunnistus- ja maksamispalvelu Vetumassa. Mobiilivarmenne on matkapuhelimen SIM-korttiin liitetty tietopaketti omistajan henkilötiedoista. Tunnistautuminen toimii käytännössä niin, että käyttäjä antaa tunnistautumista edellyttävään palveluun oman matkapuhelinnumeronsa. Palvelusta lähetetään numeroon tieto kirjautumisyrityksestä. Käyttäjä vastaa saamaansa viestiin salaisella aiemmin luodulla tunnusluvullaan. Matkapuhelin hyväksyy tunnistautumisen ja lähettää tiedon palvelulle. (Hartig 2012, hakupäivä 13.4.2013; Mobiilivarmenne 2013, hakupäivä 13.4.2013.)

2.3.2 Todennus

Henkilön todennus voi pohjautua kolmeen tekijään. Henkilö voidaan todentaa jollakin, mitä hänellä on hallussaan, esimerkiksi avain tai henkilökortti. Todentaminen voidaan tehdä myös jollain, mitä henkilö tietää, kuten esimerkiksi salasana tai PIN-koodi. Lisäksi henkilö voidaan todentaa yksilöllisellä ominaisuudella, kuten esimerkiksi ulkonäkö, ääni tai olemus. (Järvinen 2003, 35–38.)

Mikään yksittäinen todennustapa ei takaa riittävän luotettavaa todennusta, joten suurta varmuutta vaativissa sovelluksissa, kuten esimerkiksi verkkopankki, yhdistetään kaksi tai kaikki kolme eri tapaa. Pankit antavat käyttäjille käyttäjätunnuksen ja salasanan, jolloin immaterialistinen tieto on ihmisen hallussa. Lisäksi pankit jakavat asiakkailleen kertakäyttötunnuksia sisältävän listan, jolloin todennus tapahtuu henkilön hallussa olevan muuttuvien numerokoodien perusteella. (Järvinen 2003, 35–38.)

2.3.3 Hakemistopalvelu

Microsoftin Active Directory (AD) on keskitetty ja standardoitu hakemistopalvelu, joka on suunniteltu verkkoympäristöihin. Sen avulla voidaan automatisoida verkon hallinta käyttäjädatan,

turvallisuuden ja hajautettujen resurssien osalta. Active Directoryn avulla voidaan myös mahdollistaa yhteiskäyttö muiden hakemistojen kanssa. (Rouse 2008, hakupäivä 2.4.2013.)

Active Directory mahdollistaa hierarkkisen organisaatiorakenteen käyttäjätilien, laitteiden, palvelimien ja sovelluksien hallintaan. Palvelu on sisällytetty Windows 2000 server -arkkitehtuuriin mahdollistaen versioiden ylös- ja alaspäin yhteensopivuuden. (Rouse 2008, hakupäivä 2.4.2013.)

Active Directory hakemistopalvelu perustuu LDAP-protokollan (Lightweight Directory Access Protocol) määrityksiin ja voikin sanoa, että Active Directory on vain Microsoftin näkemys LDAP-käyttäjähakemistosta (Tolvanen 2011, hakupäivä 1.5.2013). LDAP-protokolla toimii TCP/IP-pinon päällä ja on rajoitetumpi versio X.500-protokollasta. LDAP-asiakasohjelmat ovat pienempiä, nopeampia ja helpompia implementoida kuin vastaavat X.500-asiakasohjelmat. LDAP käyttää nimeämiseen samanlaista tapaa kuin X.500, esimerkiksi ldap://example.com/cn=user,dc=example,dc=com. (Microsoft 2006, hakupäivä 4.5.2013.)

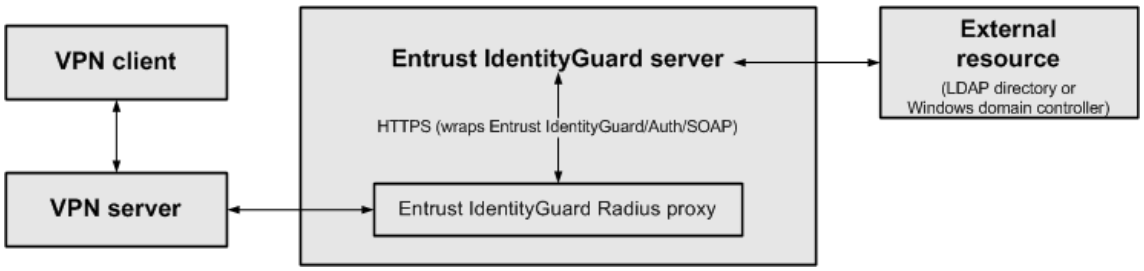
Ryhmäkäytännöt (Group Policy) ovat keinoja käyttäjien ja laitteiden hallitsemiseen tuotantoympäristössä. Ryhmäkäytännöillä voidaan kontrolloida yksittäistä käyttäjää tai konetta tai niistä muodostettua ryhmää yli tuhannen ryhmäkäytäntöobjektin avulla. (ITpro.fi 2013, hakupäivä 2.4.2013.) Ryhmäkäytännöt voidaan kohdistaa Active Directoryn toimipaikkoihin (site), toimialueisiin (domain) ja organisaatioyksiköihin (ou).

2.3.4 Välityspalvelin

Välityspalvelin kuljettaa käyttäjän kirjautumistiedon tunnistautumispalvelimelle, joka varmentaa tietokannasta käyttäjän käyttäjätunnisteen ja salasanan sekä myöntää sertifikaatin. Serifikaatin myöntämiseen tarvitaan protokolla. Kerberos on yleisesti käytetty tunnistautumisprotokolla, jonka lisäksi etätunnistautumiseen on usein käytetty protokollia RADIUS (Remote Authentication Dial-In User Service) ja TACACS+ (Terminal Access Controller Access Control System +). (Garg 2008, 205.)

RADIUS on jaettu asiakas/palvelin-järjestelmä, joka suojaa verkon luvattomalta käytöltä. Ciscon toteutuksissa RADIUS-asiakasohjelmat toimivat Ciscon reitittimillä ja ne lähettävät tunnistautumispyynnöt RADIUS-palvelimelle, joka hallitsee tiedot käyttäjätunnisteista ja verkkopalveluiden pääsyoikeuksista. (Garg 2008, 205.)

RADIUS Proxy -tunnistautumisessa (kuvio 1) VPN server lähettää tunnistautumispyynnön RADIUS-välityspalvelimelle. Välityspalvelin välittää viestin kohdepalvelimelle, jossa pyyntö varmistetaan ja vastausviesti lähetetään takaisin kohti VPN-palvelinta. (Juniper 2013, hakupäivä 29.3.2013.)



KUVIO 1. RADIUS Proxy (Entrust 2010, 8)

2.4 Salaus

Todentaminen on monessa tapauksessa aivan riittävä suojauskeino tunnistautumiseen, mutta se ei suojaa tietojen yksityisyyttä lähetettynä julkiseen verkkoon tai sen yli. Selväkielinen data on helposti kenen tahansa luettavissa. Suurimmat riskit kohdistuen salasanoihin, taloustietoihin ja luottamukselliseen informaatioon vaativat eri tekniikoiden käyttöä salata lähetetty tieto. (Farrel 2008, 118.)

Internetin salaustekniikat eivät poikkea kovin paljon hyvissä vakoiluelokuvissa näkyvistä tekniikoista. Alkuperäinen data muunnetaan mitään tarkoittamattomiksi merkeiksi jonkin algoritmin avulla. Muunnettu tieto voidaan näin turvallisesti lähettää Internetin yli vastaanottajalle, joka algoritmin avulla muuttaa tiedon takaisin selväkieliseksi. (Farrel 2008, 118.)

Salausalgoritmi luottaa siihen tosiasiaan, että viestin sieppaaja ei voi helposti purkaa salausta. Ensimmäinen menettelytapa on pitää salaus- ja purkualgoritmit salaisena. Jos algoritmit ovat hyvät, kukaan ei voi tulkata vaihdettua tietoa. Ongelmaksi muodostuu se, että salausten laajassa käytössä kaavojen täytyy olla tunnettuja. (Farrel 2008, 118.)

Ratkaisu tähän ongelmaan on käyttää avaimia. Avaimet mahdollistavat lisätiedon lisäämisen salaus- ja purkuprosesseihin tehden niistä yksilöivän, vaikka algoritmit olisivatkin laajassa tiedossa. Nämä avaimet ovat vain lähettäjän ja vastaanottajan tiedossa. (Farrel 2008, 118.)

Salaustekniikat pohjautuvat symmetriseen ja epäsymmetriseen (asymmetriseen) salaukseen. Symmetrisellä salauksella tarkoitetaan tietokoneella tehtävää bittien sekoittamista käyttäen

samaa avainta viestien salaukseen sekä purkuun. Symmetriset salaimet voidaan jakaa lohko- (block cipher) ja jonosalaimiin (stream cipher). Lohkosalain käsittelee dataa lohkoina, jotka salataan aina samalla avaimella. Jonosalain käsittelee dataa pienissä yksiköissä, bitti tai merkki kerrallaan, mutta avain vaihtuu jokaisen yksittäisen salausoperaation jälkeen. Ongelmana symmetrisessä salauksessa on avainten hallinta, sillä viestin lähettäjällä ja vastaanottajalla tulee olla tiedossaan sama salausavain. (Järvinen 2003, 77–78; Viestintävirasto 2007a, hakupäivä 1.5.2013.)

Epäsymmetrisellä salauksella tarkoitetaan viestin salaamista matemaattisella laskennalla. Julkista avainta (public key) käytetään viestin salaukseen ja yksityistä avainta (private key) käytetään viestin purkamiseen. Salausavaimet ovat erilaisia, mutta silti yhteydessä toisiinsa matemaattisella tavalla. Koska julkista avainta käytetään vain salaukseen, sen paljastumista ei tarvitse pelätä ja sitä voi levittää vapaasti. Yksityinen avain tulee taas pitää pelkästään vastaanottajan omana tietona, sillä sen paljastuessa kuka tahansa voi purkaa julkisella avaimella salatun viestin. Julkisella avaimella salattu viesti voidaan purkaa vain vastaavalla yksityisellä avaimella, jolloin edes lähettäjä ei pysty purkamaan salaamaansa viestiä. Julkisen avaimen järjestelmä poistaa symmetrisen salauksen ongelman, koska yhteistä salaisuutta ei vaadita ja avaimesta sopiminen on vain ilmoitusasia. Julkisen avaimen algoritmien heikkoutena pidetään salauksen hitautta. (Järvinen 2003, 132–133; Viestintävirasto 2007b, hakupäivä 1.5.2013.)

3 VIRTUAL PRIVATE NETWORK

Virtual Private -verkko (VPN) tarjoaa yrityksille mahdollisuuden suojata verkkojen väliset yhteydet edullisemmin käyttäen yleisiä tietoliikenneverkkoja, kuin käytettäessä erillisiä kiinteisiin linjoihin perustuvia yhteysratkaisuja. Yksityisellä virtuaaliverkolla muodostetaan yhteys fyysisesti erillään olevien tietokoneiden välille Internetin kautta. (Symantec 2013, hakupäivä 26.3.2013.) VPN-verkot mahdollistavat esimerkiksi yrityksen jaettujen hakemistojen käytön työasemassa.

VPN-verkko voidaan luoda kahden aliverkon, aliverkon ja päätelaitteen ja kahden päätelaitteen välille. Tunnelointi voidaan toteuttaa IPSec ja SSL VPN tekniikoilla. (Tibbs & Oakes 2006, 315–316.)

Verkkoliikenteen tutkiminen on mahdollista Internet-yhteyksien ollessa yleisiä ja heikosti suojattuja. VPN-verkossa tiedot voidaan salata ja luoda yksityinen ei-fyysinen verkko Internetin välityksellä. (Symantec 2013, hakupäivä 26.3.2013.)

3.1 Tunnelointi

Tunneloinnissa siirrettävä data pakataan digitaaliseen salattuun pakettiin. VPN-yhteys muodostetaan erillisellä ohjelmalla tai laitteella. Siirrettävä data salataan lähettäessä ja puretaan vastaanottaessa. (Symantec 2013, hakupäivä 26.3.2013.)

SSL VPN eroaa IPSec-yhteydestä OSI-mallin toteutuksessa. SSL VPN on toteutettu OSI-mallin kerroksilla 4–7 (kuljetus-, istunto-, esitystapa- ja sovelluskerros). (Cisco 2012, hakupäivä 28.3.2013; Wikipedia 2013, hakupäivä 27.3.2013.) IPSec toimii verkkokerroksella 3 (Wikipedia 2013, hakupäivä 27.3.2013).

IPSec VPN -yhteys soveltuu paremmin yrityksen eri toimipaikkojen väliseksi yhteydeksi, kun taas SSL VPN soveltuu yksittäisten käyttäjien yhteysmuodoksi päätelaitteen ja yrityksen verkon välille. Ylläpidon kannalta IPSec-tekniikka vaatii jokaisen VPN-verkon yhteyspisteen konfigurointia ja hallintaa. SSL VPN -tekniikassa riittää, kun hallitaan vain yhtä yhteyspistettä. (CountryVPN 2013, hakupäivä 17.4.2013.)

3.2 SSL VPN

Secure Socket Layer Virtual Private Network (SSL VPN), jota joissain tapauksissa kutsutaan myös Transport Layer Securityksi (TLS VPN). SSL version 3 ja TLS version 1 päämäärät ja tarkoitukset ovat identtiset IETF:n dokumentaatioissa. (Tibbs & Oakes 2006, 311.) IPsec VPN -yhteyteen verrattuna SSL VPN ei vaadi erikoisohjelmiston asentamista loppukäyttäjän laitteelle (Rouse 2009, hakupäivä 2.4.2013).

SSL-protokollan ominaisuuksiin kuuluu salakirjoitussarjan (cipher suite) neuvottelu, joka on kokoelma salauksen ja tunnistautumisen algoritmeja. Tiedonsiirron alkuvaiheessa yhteys alustetaan salaamattomana, jolloin tiedonsiirron aloittamiseen ei tarvita kolmansia osapuolia. SSL käyttää julkista avainta salausavaimiin ja salausavainta datan salaukseen. (Garg 2008, 204.)

Tunnelin luominen vaatii käyttäjältä ainoastaan web-selaimen, jossa tunnistautuminen suoritetaan. Loppukäyttäjän käyttöjärjestelmälläkään ei ole merkitystä tunnelin luomiseen. Useimmissa verkkoympäristöissä lähtevä HTTPS-liikenne on sallittuna. HTTPS-liikenne perustuu SSL:iin. Tämä tarkoittaa, että vaikka verkosta olisi estettynä IPSec VPN -istunnot, niin SSL VPN todennäköisesti toimii. (Cisco 2013, hakupäivä 4.5.2013.)

SSL VPN toimii sovellus- ja käyttäjäperusteisesti, jolloin verkon pääkäyttäjä voi määritellä resurssien jakamisen tarkemmin kuin VPN-yhteydessä. Pääkäyttäjä voi asettaa käyttäjille erilaisia rooleja pääsyoikeuksien suhteen ja samalla käyttäjällä voi olla erilaiset pääsyoikeudet kirjautuessaan verkkoon esimerkiksi työ- tai kotikoneeltaan. (Rissler & Root 2006, 5.)

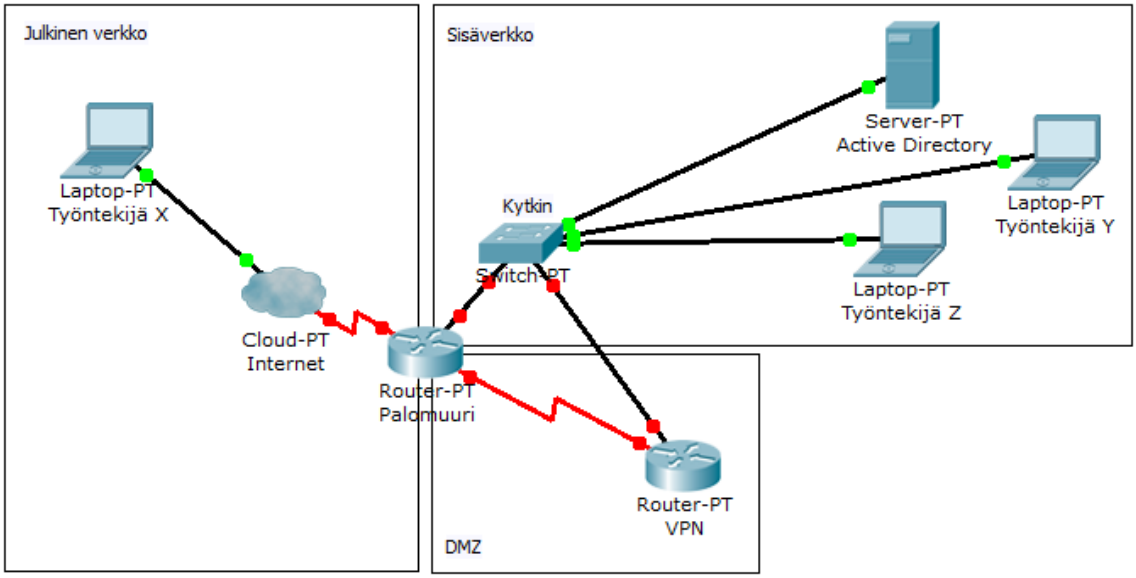
SSL VPN tarjoaa helpon tavan luoda yhteys yrityksen sisäisiin resursseihin. Tietoturva tämäntyyppisissä yhteyksissä on yhtä vahva kuin käyttäjän tunnistautuminen. Yksinkertainen käyttäjätunnus-salasanapari mahdollistaa luvattoman käytön, jos tunnistautumistiedot vain saadaan kalastettua. Tästä syystä käyttäjän tunnistamiseen on käytettävä vähintään kaksivaiheista käyttäjän todentamista. (Cisco 2013, hakupäivä 4.5.2013.)

4 KÄYTTÖÖNOTTO

4.1 Verkkoympäristö

Opinnäytetyön kohdeyrityksessä oli jo ennalta päätetty ottaa käyttöön kertakäyttösalasanajärjestelmä VPN-yhteyden tunnistautumisvaiheessa luotaessa yhteyttä yrityksen toimitilojen ulkopuolelta, julkisesta verkosta. Yrityksessä oli jo ennalta valittu kertakäyttösalasanajärjestelmäksi Entrust IdentityGuard. Järjestelmän tarkoituksena on yrityksen tietoturvapolitiikan mukainen vahva todentaminen tietojenkäsittelyssä käytettäessä sisäverkon ulkopuolisia yhteyksiä.

Yrityksessä on käytössä AD-hakemistopalvelu, palomuuri julkisen, sisäisen ja DMZ-verkon välillä sekä VPN-yhteyden mahdollistava laite, kuten kuviossa 2 ilmenee. VPN-yhteyden avulla yrityksen työntekijä voi lukea ja hallita sähköpostiaan ja tehdä osan työtehtävistään esimerkiksi kotoaan tai asiakkaan tiloista.



KUVIO 2. Verkon rakenne

4.2 Kertakäyttösalasanajärjestelmä

Entrust IdentityGuard -ohjelmisto tarjoaa lisäkerroksen jo käytössä olevan salasanakäytännön päälle, kuten esimerkiksi Active Directory, Oracle ja MySQL:n käyttäjätietokannat. Ohjelmisto

mahdollistaa vahvan tunnistautumisen yhdellä ohjelmistoalustalla useille sidosryhmille ja palveluille käyttäen eri todennustapoja, kuten erilaiset tokenit, SMS-viestit, tunnuslukulistat, älykortit tai matkapuhelimien token-ohjelmistot. Todennustapoja voidaan myös riskien minimoimiseksi yhdistää. (Salcom Group Oy 2013, hakupäivä 2.4.2013.)

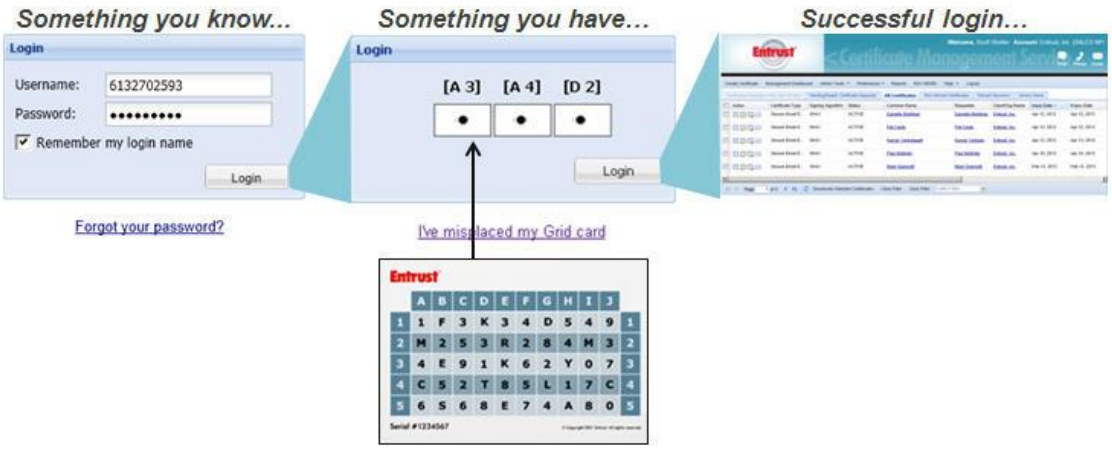
IdentityGuard-järjestelmä on jo käytössä useissa suurissakin ympäristöissä. Ruotsin työvoimatoimiston (Arbetsmarknadsverket AMV) työntekijät hyödyntävät kortilta löytyviä tunnuslukuja sähköpostin lukemisessa (Reiss 2005, hakupäivä 2.4.2013), Habbo-online-yhteisön omistaja Sulake Corporation Oy hyödyntää IdentityGuard-tokeneita (Entrust 2008, hakupäivä 4.5.2013) ja Pietarsaaren Seudun Puhelin Oy käyttää asiakkaiden vahvaan tunnistukseen asiakkaille jaettavia token-laitteita (Kauppalehti 2008, hakupäivä 2.4.2013).

Todentaminen voidaan tehdä yksi- tai kaksivaiheisesti. Yksivaiheinen todentaminen tarkoittaa tässä tapauksessa, että käyttäjältä kysytään kirjautumisen yhteydessä käyttäjätunnuksen lisäksi pelkästään tokenin tarjoama kertakäyttösalasana. Kaksivaiheinen todentaminen tarkoittaa esimerkiksi käyttäjätunnuksen ja salasanan jälkeen kysyttävää kertakäyttösalasanaa.

Grid Card

Grid Card on Entrustin patentoima taulukkomuotoinen, luottokortin kokoinen tunnistautumismenetelmä, joka sisältää numeroita ja kirjaimia. Todennus perustuu henkilön hallussa olevaan korttiin. Kortti voidaan toimittaa käyttäjälle paperisena tai esimerkiksi käyttäjän sähköpostiin.

Kirjautumisvaiheen jälkeen käyttäjälle esitetään koordinaatit, joiden perusteella käyttäjä hakee vastaavat kolme merkkiä ja ilmoittaa ne järjestelmässä esitettyyn lomakkeeseen (kuvio 3). Järjestelmä tutkii vastaavuuden käyttäjälle yhdistetyn kortin sarjanumerotunnisteen ja syötettyjen merkkien perusteella. Grid Card -menetelmää voidaan käyttää vain kaksivaiheisessa todentamisessa.



KUVIO 3. Grid Card -todentaminen (Entrust 2013, hakupäivä 13.5.2013)

Token

Kertakäyttösalasanatoken on käyttäjän hallussa oleva fyysinen laite. Token-laite voi olla esimerkiksi avaimenperäksi tehty kertakäyttösalasanalaite, joka on esitetty kuviossa 4.

Lisäksi on olemassa luottokortin kokoinen laite, joka toimii samalla periaatteella kuin token-avaimenperä. Laite kytketään päälle painonapista ja näytölle generoituu kahdeksannumeroinen salasana. Todennuspalvelimelle ilmoitetaan käyttäjän tietoihin käytettävä todennusmenetelmä (token), token-laitteen sarjanumero sekä laitteen toimittaja (Entrust).

KUVIO 4. Token

SMS-viesti

Entrust IdentityGuard mahdollistaa tekstiviestillä lähetettävän kertakäyttösalasanan käytön. Todentamisen yhteydessä käyttäjän puhelinnumeroon lähetetään normaali tekstiviesti, jonka

sisällön perusteella käyttäjä todentaa itsensä palvelulle. SMS-viesti vaatii palvelimelle laitteiston, joka on kykeneväinen lähettämään tekstiviestejä.

Tekstiviestitodennuksen etuna on laiteriippumattomuus, matkapuhelin kulkee tyypillisesti aina mukana ja Järvisen (2003, 42) esittelemä turvallisuus on myös yksi eduista GSM-verkon tietoliikennesalauksen ja PIN-koodin avulla.

Tietoon perustuva kysymys-vastaus

Käyttäjän rekisteröinnin yhteydessä käyttäjälle luodaan kysymys ja siihen soveltuva vastaus. Kysymys voi olla esimerkiksi ”ensimmäisen lemmikkisi nimi”, johon käyttäjällä on vastaus tiedossaan. Käyttäjä syöttää vastauksensa sille varattuun kenttään käyttäjätunnistautumisen jälkeen.

Salasana

Käyttäjälle voidaan asettaa toinen salasana, joka syötetään käyttäjätunnistautumisen jälkeen. Ensimmäinen todennus suoritetaan hakemistopalvelusta ja toinen todentaminen suoritetaan Entrustin tietokannasta.

Määräaikainen PIN

Järjestelmään voidaan luoda tunnus, jolle annetaan määräajan voimassa oleva PIN (Personal Identification Number). PIN-tunnukselle voidaan asettaa elinikä tunneissa tai voimassaolon päättymisaika. Tarvittaessa PIN-tunnus voidaan asettaa toistaiseksi voimassaolevaksi, jolloin tunnistautumista voidaan käyttää kuten mitä tahansa aiempaa todentamisratkaisua.

Eliniän lisäksi PIN-tunnukselle voidaan asettaa käyttörajat, jonka jälkeen tunnus lakkaa toimimasta. Oletusarvoisesti tunnuksen käyttökertoja on rajattomasti, mutta asetuksista saadaan vaihdettua tunnuksen elinikä esimerkiksi maksimissaan kolmeen tunnistautumiseen.

Soft token

Entrust mahdollistaa todentamisen myös käyttämällä mobiilisovellusta, joka toimii samalla toimintaperiaatteella kuin esimerkiksi avaimenperänä toimiva token (kuvio 5). Sovellus toimii useilla eri laitealustoilla. Googlen Play-sovelluskaupasta löytyy Android mobiilikäyttöjärjestelmälle Entrust IdentityGuard Mobile -sovellus.

Soft tokenia aktivoidessa järjestelmä antaa kaksi numerosarjaa, serial number ja activation code, jotka syötetään matkapuhelimen sovellukseen. Näiden perusteella matkapuhelinsovellus luo rekisteröintiavaimen, joka vastaavasti syötetään Entrustin järjestelmään.

KUVIO 5. Soft token -todentaminen (Entrust 2013, hakupäivä 13.5.2013)

4.3 Asennuksen vaiheet

Entrust toimittaa tuotteen mukana useita PDF-muotoisia dokumentteja tuotteen asennukseen, konfigurointeihin sekä hallintaan liittyen. Asennus voidaan suorittaa Windows tai Linux palvelimelle. Tässä käsitellään IdentityGuard-järjestelmän asentamista Windows-ympäristöön. Käyttäjätietojen haku voidaan suorittaa suoraan eri hakemistopalveluista, kuten esimerkiksi Active Directory tai erilaisista SQL-tietokannoista. Asennus vaatii AD-hakemistopalvelusta löytyvän tunnuksen, jotta IdentityGuard voidaan liittää hakemistopalveluun.

Entrust IdentityGuard Enterprise Server asennetaan palvelimelle, jossa palvelua halutaan ajaa. Asennuksen aikana luodaan ja käynnistetään Windows ympäristössä kaksi palvelua (services): Entrust IdentityGuard Server ja Entrust IdentityGuard RADIUS Proxy. Asennuspaketin suorittamisen jälkeen käyttäjälle aukeaa Entrust IdentityGuard Configuration Panel, josta käyttäjä pääsee valitsemaan käytettävän moodin, konfiguroimaan järjestelmään käyttäjätietokantayhteyden, tässä tapauksessa Active Directory, sekä initialisoi järjestelmän toimintaan.

Konfiguroinnin yhteydessä määritellään, toimiiko kyseinen palvelin primary-moodissa, jota käytetään ensiasennuksessa, vai replica-moodissa, jolloin palvelu toimii yhdessä jonkin toisen

primary-palvelimen kanssa kuormantasaajana. Konfiguroinnissa käyttäjä pääsee valitsemaan palvelun todentamisessa käytettävät portit ja selaimella käytettävän Administrator-hallintapaneelin portin.

Initialisoinnissa käyttäjä syöttää järjestelmän asennus- ja aktivointiavaimet sekä luo Master1-, Master2- ja Master3-käyttäjille salasanat. Master-käyttäjien salasanat tallennetaan *masterkeys*-tiedostoon salattuna. Master-tunnuksia käytetään järjestelmän päivityksiin, varmuuskopioiden palauttamiseen, replica-palvelimen konfigurointiin ja Master Shell komentorivipohjaiseen hallintapaneeliin. Lisäksi käyttäjä luo vielä yhden Administrator-käyttäjän, jota käytetään järjestelmän hallintaan. Tämä käyttäjä täytyy löytyä samasta hakemistopalvelusta, jonka yhteys aiemmin konfiguroitiin.

4.4 Käyttöönotto VPN-kirjautumisessa

Asentamisen ja järjestelmän initialisoinnin jälkeen voidaan järjestelmä ottaa käyttöön esimerkiksi SSL VPN -palvelinlaitteessa. Entrust IdentityGuard RADIUS Proxyn asetuksista asetetaan First-Factor -todentaminen käyttämään toimialueen hakemistopalvelua sekä luodaan yhteys VPN-laitteen välille IP-osoitteen sekä jaetun salausavaimen perusteella.

Vastaava IP-osoite, porttinumero ja jaettu salausavain asetetaan myös SSL VPN -laitteen asetuksiin. SSL VPN -laitteen asetuksista täytyy asettaa päälle kertakäyttösalasanajärjestelmän käyttäminen, jolloin kirjautumisvaiheessa laite ymmärtää pyytää käyttäjätunnuksen ja salasanan lisäksi asetetun ylimääräisen tunnistetiedon.

5 HALLINTA

5.1 Käyttäjän lisääminen järjestelmään

Käyttäjä lisätään IdentityGuard-järjestelmään selainpohjaisen Administration-hallintapaneelin kautta. Käyttäjä lisätään samalla käyttäjätunnuksella kuin Active Directory -hakemistopalvelussa. Käyttäjän lisäämisen yhteydessä IdentityGuard-järjestelmä hakee hakemistopalvelusta käyttäjän lisätietoja, kuten koko nimi, puhelinnumero sekä sähköpostiosoite, kuten kuvio 6 osoittaa.

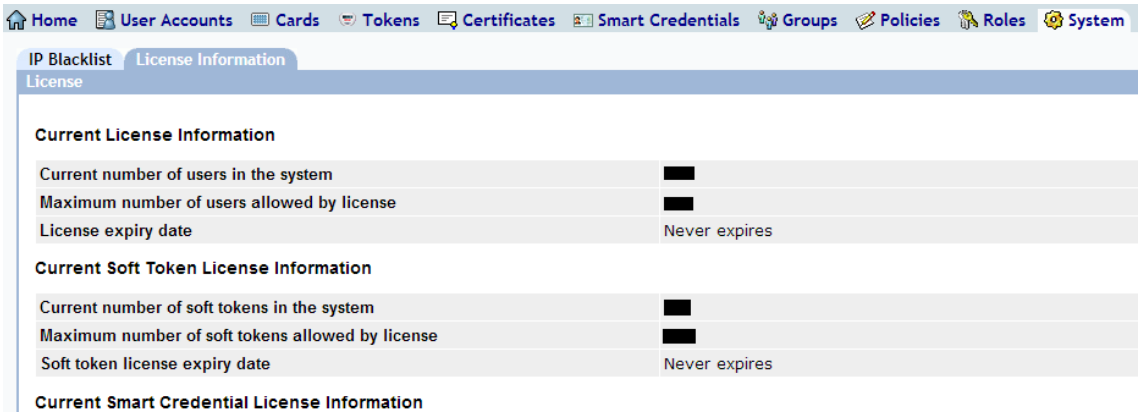
KUVIO 6. IdentityGuard-järjestelmän hakemat tiedot Active Directorystä ja käyttäjälle osoitettu token-laite

Kun käyttäjä on onnistuneesti lisätty, voidaan hänelle osoittaa jokin tunnistautumismenetelmä, kuten esimerkiksi token-laite tai Grid Card. Kun token-laite on yhdistetty käyttäjän profiiliin, synkronoidaan kaksi laitteen peräkkäin antamaa kertakäyttösalasanaa järjestelmään. Toimenpiteen jälkeen token-laite on käyttövalmis ja työntekijän kirjautumisen yhteydessä kysytään hänelle osoitetun token-laitteen antamaa kertakäyttösalasanaa. Grid Cardia ei tarvitse synkronoida järjestelmään, vaan sen osoittamat merkit määräytyvät kortin sarjanumeron perusteella.

5.2 Lisenssitietojen tarkastaminen

Järjestelmän ylläpitäjän täytyy tietää järjestelmän lisenssien määrä ja voimassaoloaika, jotta esimerkiksi yrityksen työntekijämäärän kasvaessa uudetkin työntekijät saavat pääsyn yrityksen resursseihin. Nämä tiedot löytyvät samasta IdentityGuard Administration -hallintapaneelista, jossa käyttäjien lisääminen tapahtuu.

Lisenssivälilehti kertoo tiedot järjestelmään liitettyjen käyttäjien määrästä, maksimimäärästä ja lisenssin voimassaoloajan. Samat tiedot esitetään käyttäjien, soft tokeneiden ja smart credentialien osalta (kuvio 7).



KUVIO 7. License Information

6 POHDINTA

Opinnäytetyön tarkoituksena oli parantaa yrityksen tietoturvan tasoa luomalla vahva todennus julkisen verkon yhteyksistä sisäverkon resursseihin. Työn toiminnallinen osuus sujui suunnitellusti ja yritys sai käyttöönsä toimivan kertakäyttösalasanajärjestelmän. Järjestelmää on helppo muokata yrityksen tarpeiden mukaan ja laajentaa vahvaa todentamista myös muihin yrityksen todennustapahtumiin. Järjestelmä otetaan käyttöön kaikille yrityksen työntekijöille, koska kaikki käyttäjät tukeutuvat tietoturvapolitiikan mukaiseen vahvaan todentamiseen.

Työ onnistui suunnitellusti ja ennakkoaikataulut pitivät paikkaansa lähes poikkeuksetta. Järjestelmän asennus onnistui ohjeita noudattaen mukaillen niitä yrityksen olemassa olevaan verkkoinfrastruktuuriin. Opinnäytetyön tuloksena saatiin helposti muokattava ja hallittava järjestelmä yrityksen käyttöön. IT-henkilökunnalla ja yrityksen muulla henkilöstöllä on kohtuullisen pieni kynnys opetella käyttöönotetun järjestelmän käyttö, koska se on hyvin jo ohjelmistotoimittajan puolesta ohjeistettu ja looginen käyttää. Yrityksen työntekijöille muutos näkyy käytännössä pelkästään sisäänkirjautumisen yhteydessä tulevassa vaiheessa, jolloin kertakäyttösalasanaa kysytään.

Toimeksiantaja oli jo valmiiksi päätynyt Entrust IdentityGuard -järjestelmään. Vastaavanlaisen järjestelmän toteuttamiseen olisi voitu valita RSA:n toimittama SecurID ja McAfeen toimittama One Time Password. RSA:n järjestelmä on lähes identtinen Entrustin järjestelmän kanssa. McAfeen järjestelmä tarjoaa mahdollisuuden käyttää vain Soft Tokeneita.

Direct Access (DA) on myös yksi potentiaalinen vaihtoehto toteuttaa VPN:n kaltainen yhteys. DA toimii Microsoftin Server 2008 R2 ja Windows 7 -käyttöjärjestelmissä sekä niiden jälkeen julkaistuissa käyttöjärjestelmissä. Etu käytettäessä DA:ia on, että käyttäjän työasema ottaa yhteyden sisäverkon resursseihin samalla kun kone saa Internet-yhteyden. Kohdeyrityksen toimintaan Direct Access voisi olla yksi vaihtoehto, mutta nykyisellä SSL VPN -järjestelmällä saadaan paremmin rajattua resursseja. SSL VPN edellyttää hieman käyttäjätoimia kirjautumisessa, mutta yrityksen työntekijät ovat jo tähän tottuneet eikä kahden samankaltaisen järjestelmän ylläpitäminen ole kannattavaa.

Direct Access -järjestelmään voi lisätä kertakäyttösalasanatodentamisen samaan tapaan kuin nykyiseen SSL VPN -ratkaisuun. Tässä ratkaisussa työntekijä todennetaan ensin Direct Access

Serverillä hakemistopalvelusta, jonka jälkeen käytetään kertakäyttösalasanapalvelinta kertakäyttöisen salasanan tarkistamiseen.

Entrust IdentityGuard -järjestelmän voisi ottaa tulevaisuudessa käyttöön myös muissa yrityksen todentamisissa. Lisäksi Entrustilla on muita tuotteita, kuten esimerkiksi Single Sign-On (SSO) kertakirjautumisjärjestelmä Entrust GetAccess. SSO-järjestelmän ideana on sujuvoittaa useiden samaa käyttäjätunnustietokantaa käyttävien järjestelmien käyttöä. Tässä operaatiossa käyttäjät pääsevät käyttämään useita eri palveluita yhdellä todentamisoperaatiolla.

LÄHTEET

Cibernarium 2005. Käyttäjätunnus ja salasana. Hakupäivä 2.4.2013, http://www.cibernarium.tamk.fi/tietoturva2/salasana.htm.

Cisco 2012. Internetworking Basics. Hakupäivä 28.3.2013, http://docwiki.cisco.com/wiki/Internetworking_Basics.

Cisco 2013. SSL VPN Security. Hakupäivä 4.5.2013, http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html.

CountryVPN 2013. Short Comparison Between IPSec VPN And SSL VPN. Hakupäivä 17.4.2013, http://www.countryvpn.com/short-comparison-between-ipsec-vpn-and-ssl-vpn/.

Entrust 2008. Finland-based Sulake to Deploy Entrust Versatile Authentication Platform to Authenticate Remote Access Users. Hakupäivä 4.5.2013, http://www.entrust.com/news/index.php?s=27003&item=73013.

Entrust 2010. Technical Integration Guide for Entrust IdentityGuard 9.2 and Juniper Networks Secure Access SSL VPNs. Hakupäivä 29.3.2013, http://download.entrust.com/resources/download.cfm/22233/.

Entrust 2013. Multifactor Authentication to CMS. Hakupäivä 13.5.2013, http://www.entrust.net/certificate-services/cms-authentication.htm.

Farrel, A. 2008. Concepts in IP Security. Teoksessa Network security: know it all. Burlington: Morgan Kaufman Publishers, 107–148.

Garg, V. 2008. Security in Wireless Systems. Teoksessa Network security: know it all. Burlington: Morgan Kaufman Publishers, 175–210.

Google Play 2012. Entrust IdentityGuard Mobile. Hakupäivä 11.5.2013, https://play.google.com/store/apps/details?id=com.entrust.identityGuard.mobile.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo Finland Oy.

Hartig, O. 2012. Kännykällä tunnistautuminen tulee vihdoinkin. Hakupäivä 13.4.2013, http://www.tietoviikko.fi/cio/kannykalla+tunnistautuminen+tulee+vihdoinkin/a801687.

Hämäläinen, P. 2005. Yrityksen tietoturvapolitiikka. Hakupäivä 24.3.2013, http://www.tietokone.fi/lehti/tietokone_1_2005/yrityksen_tietoturvapolitiikka_2610.

ITpro.fi 2013. Aktiivihakemisto. Hakupäivä 2.4.2013, http://itpro.fi/wiki/sivut/Identiteetti%20ja%20hakemistot/Active%20Directory.aspx.

Juniper Networks, Inc. 2013. Proxy RADIUS Overview. Hakupäivä 29.3.2013, http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/ProxyTargets2.html.

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo Finland Oy.

Kauppalehti 2008. RAXCO FINLAND: Pietarsaaren Seudun Puhelin tarjoaa vahvaa tunnistusta ITC-palveluna. Hakupäivä 2.4.2013, http://www.kauppalehti.fi/5/i/yritykset/lehdisto/hellink/tiedote.jsp?oid=20081201/12289017931410.

McCabe, J. 2008. Security and Privacy Architecture. Teoksessa Network security: know it all. Burlington: Morgan Kaufman Publishers, 65–86.

Microsoft 2012. Passwords Technical Overview. Hakupäivä 28.5.2013, http://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx.

Microsoft 2006. Introduction to Lightweight Directory Access Protocol (LDAP). Hakupäivä 4.5.2013, http://support.microsoft.com/kb/196455.

Mobiilivarmenne 2013. Usein kysytyt kysymykset. Hakupäivä 13.4.2013, http://www.mobiilivarmenne.fi/fi/faq/.

Reiss, M. 2005. Ruotsin työvoimatoimisto nojaa Pointseciin. Hakupäivä 2.4.2013, http://www.digitoday.fi/tietoturva/2005/02/16/ruotsin-tyovoimatoimisto-nojaa-pointseciin/20058216/66.

Rissler, R. & Root, D. 2006. IPSec and SSL VPN Decision Criteria. Hakupäivä 27.3.2013, http://ebookbrowse.com/juniper-ipsec-vs-ssl-vpn-pdf-d319285818.

Rouse, M. 2008. Active Directory. Hakupäivä 2.4.2013, http://searchwindowsserver.techtarget.com/definition/Active-Directory.

Rouse, M. 2009. SSL VPN (Secure Sockets Layer virtual private network). Hakupäivä 2.4.2013, http://searchsecurity.techtarget.com/definition/SSL-VPN.

Salcom Group Oy 2013. Entrust IdentityGuard. Hakupäivä 2.4.2013, http://www.salcom.fi/inet/salcom/flow.nsf/docs/Entrust_IdentityGuard.

Sanastokeskus TSK ry 2004. Tiivis tietoturvasanasto. Hakupäivä 2.4.2013, http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf.

Symantec 2013. VPN-opas. Hakupäivä 26.3.2013, http://www.symantec.com/region/fi/resources/vpn.html.

Oulun yliopisto: Tietohallinto 2013. Yleisesti tietoturvasta. Hakupäivä 13.4.2013, http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoturvasta.html.

Tibbs, R. & Oakes, E. 2006. Firewalls and VPNs: Principles and Practices. New Jersey: Pearson Education, Inc.

Tietoturvaopas.fi 2013. Yrityksen tietoturvaopas. Hakupäivä 2.4.2013, http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html.

Tolvanen, P 2011. Käsitteet ojennukseen: Active Directory (AD), LDAP, SSO ja identiteetinhallinta. Hakupäivä 1.5.2013, http://viidestaso.wordpress.com/2011/04/29/kasitteet-ojennukseen-active-directory-ad-ldap-sso-ja-identiteetinhallinta/.

Valtiovarainministeriö 2012. Verkkopalvelujen laatukriteeristö - Väline julkisten verkkopalvelujen kehittämiseen ja arviointiin. Hakupäivä 13.4.2013, http://www.suomi.fi/suomifi/tyohuone/laatua_verkkoon/laatukriteeristo/uusi_kriteeristo/Verkkopalvelujen_laatukriteerist_4a_2012.pdf.

Viestintävirasto 2007a. Symmetrinen salaus. Hakupäivä 1.5.2013, http://web.archive.org/web/20101122165623/http://ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/symmetrinensalaus.html.

Viestintävirasto 2007b. Epäsymmetrinen salaus. Hakupäivä 1.5.2013, http://web.archive.org/web/20101122000805/http://ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/epasymmetrinensalaus.html.

Wikipedia 2013. SSL VPN. Hakupäivä 27.3.2013, http://fi.wikipedia.org/wiki/SSL_VPN.